(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/22666 A1

(51) International Patent Classification[7]: H04L 12/56, 29/06

(21) International Application Number: PCT/SE00/01712

(22) International Filing Date:
6 September 2000 (06.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9903390-4 20 September 1999 (20.09.1999) SE

(71) Applicant: TELEFONAKTIEBOLAGET L M ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: BRANDT, Harald; Haeffnersvägen 18, S-129 38 Hägersten (SE). HARASZTI, Zsolt; 2323 Trellis Green, Cary, NC 27511 (US). CASTRO, Rui; R. Costa Cabral, 906-3, P-4200-213 Porto (PT).

(74) Agent: DR. LUDWIG BRANN PATENTBYRÅ AB; Box 171 92, S-104 62 Stockholm (SE).

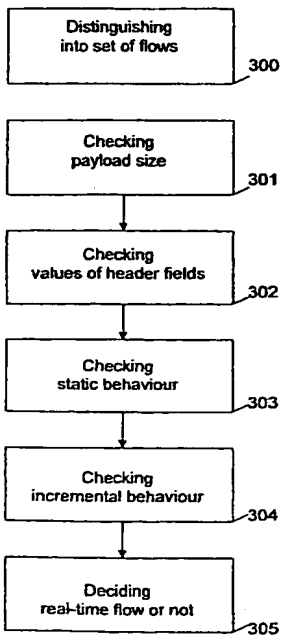
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: IP FLOW CLASSIFIER FOR DISTINGUISHING REAL-TIME FLOWS FROM NON-REAL-TIME FLOWS



(57) Abstract: The present invention relates to the requirement of differentiated service to real time packets and other type of packets, in an IP network. More particularly it relates to the problem with unacceptable latency in the network resulting in real-time packet being useless to the receiver. A problem for a node is to know whether a received datagram comprises real-time data or not. An aggregated flow within an IP network passes through a Flow Classifier before entering a node. The Flow Classifier distinguishes the aggregated flow into set of flows, each corresponding to an uni-directional packet stream from a single session. The Flow Classifier executes at least one of the following checkings: checking payload size, checking for static behaviour in header fields that are predictably constant if the flow is a real-time flow or checking for incremental behaviour of header fields, which predictably increment if the flow is a real-time flow. Based on these checkings, the Flow Classifier decides whether the flow is a real-time flow or non-real-time flow.

WO 01/22666 A1

IP FLOW CLASSIFIER FOR DISTINGUISHING REAL-TIME FLOWS FROM NON-REAL-TIME FLOWS

FIELD OF INVENTION

The present invention relates to the field of IP (Internet Protocol) networks and more specifically to an IP network, a Flow Classifier and a method for classifying IP flows in an IP network.

DESCRIPTION OF RELATED ART

Data networks for transferring electronic information are becoming increasingly widespread for the communication of many different types of data including text, graphics, voice and video data used with a computer. Such networks enable the interconnection of large numbers of computer workstations, telephone and television systems, video teleconferencing systems and other facilities over common data links or carriers.

Protocols between communicating computer systems are often implemented at multiple layers of a structural model. TCP/IP (Transport Control Protocol/Internet Protocol) and UDP/IP (User Datagram Protocol/Internet Protocol) are used to communicate across any set of interconnected networks. The TCP/IP and the UDP/IP software are both organised into four conceptual layers that are built on a fifth layer, the hardware. The highest layer is the application layer, followed by the transport layer, the network layer, the data link layer and the physical layer, which is the hardware layer. For example the physical layer uses various transport medium, and the data link layer insures that the individual data packets are not corrupted during transmission between two directly connected systems. In TCP/IP the network and transport layers ensure that data packets arrive at the correct systems within a network and in a correct order. UDP/IP does not correct corrupted packets and does not ensure that the data packets arrive in a correct order. IP is a network protocol and TCP and UDP are transport protocols. Higher layers also talk to one another using various preselected protocols, for example RTP (Real time Transfer Protocol) which is a protocol for

the transport of real-time data. Real-time data is a form of data where the correctness of the received packets depends not only on the logical result of the received data but also on the time at which the data arrives, such as audio and video. RTP is typically used over UDP. When transferring real-time data, using RTP and UDP protocols over an IP network the real-time data is broken up into frames. To keep track of details, such as frame sequence and timing, RTP attaches a header to each frame and hands over the resulting RTP frame (RTP header + frame) to UDP. UDP then adds its own header to the RTP frame = UDP datagram and hands it over to IP. IP then adds its own header to the UDP datagram = IP datagram. The resulting packet of data appears to be real-time data + RTP header + UDP header + IP header.

The specification documents of the Internet protocol suite, as defined by the IETF (Internet Engineering Task Force) and its steering group (the IESG), are published as RFCs (Requests for Comments).

In conventional IP networks, protocol layers operate in a rather isolated mode. For example, the transport layer offers the same service to all applications. Vice versa, applications operate independently of the characteristics, e.g. bandwidth and packet loss rate, of the underlying transport network.

A problem is that a too long time delay in situations of temporary overload in a node makes real-time data, such as audio or video useless but does not cause corresponding damages to other types of data. This problem would be alleviated if real-time data were prioritised over non-real-time data. In this case and other cases where service differentiation is crucial, it is required that the server entity can distinguish between packets with different service demands. Often, one base of the differentiation is application category and/or different protocol format used by the flow. This assumes that the node in order to distinguish between packets with different service demands must know the type of application and/or protocol. For example the use of RTP protocol points out that the flow is a real-time flow and shall in case of temporary overload be prioritised over non-real-time flow.

Other examples of where service differentiation is required based on whether real-time data or other types of data is transferred are:

-when an outgoing link of a node is a radio link, where the allocation of radio recourses depends on whether the transmitted data is real-time data or non-real-time data,

-requesting the link layer to recover from errors, which is not required for real-time data but for other types of data, and

-access to a server or to a network.

When protocol units are encapsulated in other lower-layer protocol units, a convenient way to identify the type of the encapsulated protocol is to use an explicit field in the header of the encapsulating lower-layer (e.g. IP) protocol. This is implemented in IP version 4 and IP version 6. This explicit field is the so-called TOS (Type Of Service) field and the network nodes that implement the differentiated services enhancements to IP use a codepoint in the IP header to select a PHB (Per-Hop Behaviour) as the specific forwarding treatment for that packet. This is described in the RFC 2598.

Thus, by reading this field, any unit that processes the packet flow can easily learn the type of the encapsulated protocol. Unfortunately, this explicit information is not commonly used.

The UDP header and TCP header do not carry any explicit information that can tell a receiving node that its payload contains real-time data.

U.S. patent no. 5 903 735 describes a method and apparatus of transmitting time critical messages over a network path having a plurality of nodes. The data is classified as minimal bandwidth data in the first node and prioritised over other data without minimal bandwidth requirements when transmitted. The higher priority is maintained by the plurality of nodes of the network path.

The problem is solved by bandwidth reservation through the path. This is, of course, a waist of bandwidth during those periods when less than the full bandwidth is required.

Therefore, what is further needed is a mechanism for classifying a flow as being a real-time flow or not, without explicit protocol format identifiers, without explicit flow description messages and without unnecessary waist of bandwidth.

SUMMARY OF THE INVENTION

The present invention relates to the requirement of differentiated service to real time packets and other type of packets, in an IP network. More particularly it relates to the problem with unacceptable latency in the network resulting in real-time packet being useless to the receiver.

A problem for a node is to know whether a received datagram comprises real-time data or not.

Accordingly, it is an object of the present invention to unravel the above-mentioned problems.

The aforesaid problems are solved by means of an IP network wherein a series of checkings in the headers of a flow classifies the flow as being a real-time flow or non-real-time flow.

The following scenario of classifying a flow describes the inventive concept of the present invention.

An aggregated flow within an IP network passes through a Flow Classifier before entering a node. The Flow Classifier distinguishes the aggregated flow into set of flows, each corresponding to an uni-directional packet stream from a single session. The Flow Classifier executes at least one of the following checkings on each flow:

- checking payload size,
- checking for static behaviour in header fields that are predictably constant if the flow is a real-time flow or

- checking for incremental behaviour of header fields, which predictably increment if the flow is a real-time flow.

Based on these checkings, the Flow Classifier decides whether the flow is a real-time flow or non-real-time flow.

An advantage of the present invention is that the real-time flow will be faster transferred over the network.

Another advantage of the invention is that network recourses will be more efficiently used.

Yet an advantage of the present invention is that real-time data is identified independently of whether explicit description (e.g. by means of signalling) of the real-time flow is available or not.

Another advantage of the present invention is that, when it is used in radio access networks for detecting IP packet flows with real-time requirements, the resource allocation can then be optimised. This improves the network utilisation and the service quality perceived by the user.

Further scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows an RTP header.

Figure 2 shows an overview of an IP network according to the invention.

Figure 3 shows a flowchart of the general method of the invention.

DESCRIPTION OF PREFFERED EMBODIMENTS

An RTP header will now be described according to RFC 1889 section 5, to simplify the understanding of the preferred embodiments. The RTP protocol unit header has some predictable properties that make it possible to test a UDP flow and tell if it contains RTP frames or not. However, the invention is not merely applicable to RTP flows only, it is applicable to other protocol formats that have similar predictable header behaviour. The format of the RTP header is shown in figure 1. The fields have the following meaning:

Version V: 2 bits

This field identifies the version of RTP. The version defined by this specification is two (2).

Padding P: 1 bit

If the padding bit is set, the packet contains one or more additional padding octets at the end which are not part of the payload. The last octet of the padding contains a count of how many padding octets should be ignored. Padding may be needed by some encryption algorithms with fixed block sizes or for carrying several RTP packets in a lower layer protocol data unit.

Extension X: 1 bit

If the extension bit is set, the fixed header is followed by exactly one header extension, with a format defined in section 5.3.1 in the RFC mentioned above.

CSRC count CC: 4 bits

The CSRC (synchronisation source) count contains the number of CSRC identifiers that follow the fixed header.

Marker M: 1 bit

The interpretation of the marker is defined by a profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream. A profile may define additional marker bits or specify that there is no marker bit by changing the number of bits in the payload type field. This is further described in section 5.3 in the RFC mentioned above.

Payload type PT: 7 bits

This field identifies the format of the RTP payload and determines its interpretation by the application. A profile specifies default static mapping of payload type codes to payload formats. Additional payload type codes may be defined dynamically through non-RTP means, which is further described in section 3 in the RFC mentioned above. An initial set of default mappings for audio and video is specified in the companion profile Internet-Draft draft-ietf-avt-profile, and may be extended in future editions of the Assigned Numbers RFC. An RTP sender emits a single RTP payload type at any given time; this field is not intended for multiplexing separate media streams.

Sequence number SN: 16 bits

The sequence number increments by one for each data packet sent, and may be used by the receiver to be detect packet loss and to restore packet sequence. The initial value of the sequence number is random (unpredictable) to make known-plaintext attacks on encryption more difficult, even if the source itself does not encrypt, because the packets may flow through a translator that does.

Timestamp TS: 32 bits

The timestamp reflects the sampling instant of the first octet in the RTP data packet. The sampling instant must be derived from a clock that increments monotonically and linearly in time to allow synchronisation and jitter calculations (see further in section 6.3.1 in the RFC mentioned above)

The resolution of the clock must be sufficient for the desired synchronisation accuracy and for measuring packet arrival jitter (one tick per video is typically not sufficient). The clock frequency is dependent on the format of data carried as payload and is specified statically in the profile or payload format specification that defines the format, or may be specified dynamically for payload formats defined through non-RTP means. If RTP packets are generated periodically, the nominal sampling instant as determined from the sampling clock is to be used, not a reading of the system clock. As an example, for fixed-rate audio the timestamp clock would likely increment by one for each sampling period. If an audio application reads blocks covering 160 sampling periods from the input device, the timestamp would be increased by 160 for each such block regardless of whether the block is transmitted in a packet or dropped as silence.

Synchronisation source SSRC: 32 bits

The SSRC field identifies the synchronisation source. This identifier is chosen randomly, with the intent that no two synchronisation sources within the same RTP session will have the same SSRC identifier. An example algorithm for generating a random identifier is presented in Appendix A.6 in the above mentioned RFC. Although the probability of multiple sources choosing the same identifier is low, all RTP implementations must be prepared to detect and resolve collisions. If a source changes its source transport address, it must also choose a new SSRC identifier to avoid being interpreted as a looped source.

Contributing source CSRC list: 0-15 items, 32 bits each

The CSRC list identifies the contributing sources for the payload contained in this packet. The number of identifiers is given by the CC field. If there are more than 15 contributing sources, only 15 may be identified. CSRC identifiers are inserted by mixers, using the SSRC identifiers of contributing sources. For example, for audio packets the SSRC identifiers of all sources

that were mixed together to create a packet area listed, allowing correct talker indication at the receiver.

In figure 2 the preferred embodiment of the IP network 200 in which services are differentiated based on whether a transmitted flow 201, 202, 203 is a real-time flow or not. The IP network 200 comprises interconnected nodes 204 representing for example, switches, routers and hosts. An aggregated flow is defined as a mix of all the different flows being transferred over a point in the IP network 200, each flow corresponding to an uni-directional packet stream of IP datagram from a single session. Aggregated flows are transferred in the IP network 200 between the nodes 204. The IP network 200 also comprises Flow Classifiers 205 through which an aggregated flow 201, 202 passes before entering a node 204. A Flow Classifier 205 can also be co-located in a node 204.

The Flow Classifier 205 has means 206 for distinguishing the incoming aggregated flow 201 into a set of flows, each flow corresponding to an uni-directional packet stream of IP datagram from a single session. This distinguishing makes it possible for the Flow Classifier 205 to look at a flow from a single session at a time.

The Flow Classifier 205 also has means 207 for checking payload size of the transport layer datagram of a packet in a flow of a particular session and also means 213 for checking if the payload size of the transport layer datagram is larger than the smallest possible datagram of a specific session comprising real-time data. If it is, it might be a real-time flow, but if it is not, it is not a real-time flow. For example, checking if the UDP payload size is larger than the smallest possible RTP frame.

The Flow Classifier 205 also has means 208 for looking at a number of consecutive data packets in the flow of the specific session and checking for static behaviour in the header fields, which are predictably constant if the flow of the particular session is a real-time flow. For example, check if the header fields, that

are supposed to be constant in consecutive RTP frames within a session, are constant in the investigated flow. Examples of constant RTP header fields are the version V field and the payload PT field. The payload type PT field tells what is inside RTP, such as if it is GSM codec, if it is voice or if it is something else. These are constant during the session if it is a real-time flow. If these header fields in the investigated flow are not constant, it is a non-real-time flow.

The Flow Classifier 205 also has means 209 for looking at a number of consecutive data packets in the flow of the specific session and checking incremental behaviour of header fields, which are predictably incremented if the flow of a particular session is a real-time flow. For example, checking in the possible RTP header if the fields that are supposed to be incremented, according to above mentioned RFC 1889, are incremented. Examples of incrementing RTP header fields are the sequence number SN field and the timestamp TS field. If these header fields, that are supposed to be incremented in the investigated flow, are not incremented, it is a non-real-time flow.

The Flow Classifier 205 further has means 212 for checking if the values of the header fields of an application datagram satisfy the range restrictions of the header of an application datagram comprising real-time data, e.g. an RTP frame. If the range restrictions are not satisfied in the investigated flow, it is not a real-time flow.

The Flow Classifier 205 further has means 210 for deciding whether the flow is a real-time flow or not, based on the previous checkings. When looking at a number of consecutive data packets in the flow, consideration has to be taken that some packet or packets might be missing.

The Flow Classifier 205 has means 211 for reporting the decision whether the flow is a real-time flow or not to the node 204.

In one embodiment of the present invention, an outgoing link 203 of the node 204 constitutes a radio link and the node 204 has means 214 for allocating radio resources on basis of the flow being a real-time flow or not.

In another embodiment, the node 204 has means 215 to request the link layer to either recover from errors if the flow is a non-real-time flow or not recover from errors if the flow is a real-time flow. There is no requirement for recovering from errors when transferring real-time data.

In yet another embodiment, the node 204 constitutes a switch. The switch has means 216 for prioritising a real-time flow over non-real-time flow when switching, e.g. in situations of temporary overload.

In yet another embodiment, the node 204 constitutes a router. The router has means 216 for prioritising a real-time flow over non-real-time flow when routing, e.g. in situations of temporary overload.

Figure 3 shows a flowchart of a possible scenario of distinguishing a real-time flow from other types of flows in a stream of IP packets in an IP network 200. The IP network 200 comprises interconnected nodes 204. Aggregated flows are transferred in the IP network 200 between the nodes 204. The node 204 has accordingly an incoming aggregated flow of IP datagram. The incoming aggregated flow is distinguished 300 into a set of flows, where each flow corresponds to an uni-directional packet stream from a single session. This makes it possible to look at a flow from a single session at a time.

The method then comprises at least one of following checkings:

- *Checking* payload size 301 of the transport layer datagram of a packet in a flow of a particular session. In one embodiment it is also possible to check if the payload size of the transport layer datagram is larger than the smallest possible datagram of a specific session comprising real-time data, e.g. checking if the

UDP payload size is larger than the smallest possible RTP frame. If it is, it might be a real-time flow. If it is not, it is not a real-time flow.

- *Checking* if the values of the header fields of an application datagram satisfy the range restrictions 302 of the header of an application datagram comprising real-time data, e.g. an RTP frame. If the range restrictions are not satisfied in the investigated flow, it is not a real-time flow.
- Looking at a number of consecutive data packets in the flow of the specific session and *checking* for static behaviour 303 in the header fields that are predictably constant if the flow of the particular session is a real-time flow. For example checking if the header fields that are supposed to be constant in consecutive RTP frames within a session are constant in the investigated flow. Examples of constant RTP header fields are the version V field and the payload PT field. The payload type PT field tells what is inside RTP such as if it is from a GSM codec, if it is voice or if it is something else. These are constant during the session if it is real-time. If these header fields in the investigated flow are not constant, it is not a real-time flow.
- Looking at a number of consecutive data packets in the flow of the specific session and *checking* incremental behaviour 304 of header fields, which are predictably incremented if the flow of a particular session is a real-time flow. For example checking in the possible RTP header if the fields that are supposed to be incremented, according to above mentioned RFC 1889, are incremented. Examples of incrementing RTP header fields are the sequence number SN field and the timestamp TS field. If these header fields that are supposed to be incremented in the investigated flow are not incremented, it is not a real-time flow.

The method comprises the further step of deciding 305 whether the flow is a real-time flow or not, based on the previous checkings.

The performed checkings are each resulting in either non-real-time flow or possible real-time flow. If one of the checking steps above shows that it is non-

real-time data, then no more checkings are required. An example of how these checkings can be performed will now be described:

First, checking if the payload size of the UDP payload size is larger than the smallest possible RTP frame. If it is not, the flow is classified as a non-real-time flow. If it is, it might be a real-time flow and further checkings are required.

If so, follows a checking if the values of the header fields of an application datagram satisfy the range restrictions 302 of an RTP header. If the range restrictions are not satisfied in the investigated flow, the flow is classified as a non-real-time flow. If they are satisfied it might be a real-time flow and further checkings are required. In that case next step is to check if the header fields that are supposed to be constant in consecutive RTP frames within a session are constant in the investigated flow. If they are not constant, the flow is classified as a non-real-time flow. If they are constant, it is a possible real-time flow and further checking is required.

In that case, checking in the possible RTP header if the fields, that are supposed to be incremented in consecutive RTP frames according to above mentioned RFC 1889, are incremented. If these header fields are not incremented, the flow is classified as a non-real-time flow. On the other hand, if these header fields are incremented, the flow is classified as a real-time flow.

When looking at a number of consecutive data packets in the flow and checking for incremental behaviour, consideration has to be taken into that some packet or packets might be missing.

In one embodiment the method comprises a step of reporting the decision whether the flow is a real-time flow or not, to the node 204.

CLAIMS

1. An IP network (200) having service differentiation based on whether a transmitted flow (201, 202, 203) is a real-time flow or not, the IP network (200) comprising a node (204) receiving an incoming aggregated flow (201) of IP datagram via a Flow Classifier (205), **characterised** by the Flow Classifier (205) having;

   - means (206) for distinguishing the aggregated flow into at least one set of flows, each flow corresponding to a uni-directional packet stream from a particular session,

   and the Flow Classifier (205) having at least one of the following means;

   - means (207) for checking the payload size of the transport layer datagram of a packet in a flow of a particular session;
   - means (208) for checking for static behaviour in header fields, of a number of consecutive data packets in the flow of the particular session; or
   - means (209) for checking for incremental behaviour of header fields, of a number of consecutive data packets in the flow of the particular session; and

   the Flow Classifier (205) further having:

   - means for performing one of said checkings;
   - means for performing a further one of the not yet performed said checkings, if said performed first checking results in that the flow possible is a real-time flow;
   - means for performing a yet further one of the not yet performed said checkings and so on until all said checkings are performed,
   - means for deciding that the flow is a real-time flow, if the last performed checking step results in that the flow possible is a real time flow.

2. The IP network according to claim 1, **characterised** in Flow Classifier (205) comprising means (211) for reporting to the node (204) whether the flow is real-time flow or not.

3. The IP network (200) according to any of the claims 1 and 2, **characterised** by the Flow Classifier (205) having means (212) for checking if the values of the header fields of an application datagram in a flow of a particular session satisfy range restrictions for a header of an application datagram comprising real-time data.

4. The IP network (200) according to any of the claims 1-3, **characterised** by the Flow Classifier (205) having means (213) for checking if the payload size of the transport layer datagram is at least as large as the smallest possible datagram of any session comprising real-time data.

5. The IP network (200) according to any of the claims 1-4, wherein an outgoing link (203) of the node (204) is a radio link, **characterised** by the node (204) having means (214) for allocating at least one radio resource on basis of the flow being a real-time flow or not.

6. The IP network (200) according to any of the claims 1-5, **characterised** by the node (204) having means (215) for requesting the link layer to recover from errors if the flow is non-real-time flow.

7. The IP network (200) according to any of the claims 1-5, **characterised** by the node (204) having means for requesting (215) the link layer not to recover from errors if the flow is a real-time flow.

8. The IP network (200) according to any of the claims 1-4, wherein the node (204) is a switch, **characterised** by the switch having means (216) for prioritising a real-time flow over non-real-time flows when switching.

9. The IP network (200) according to any of the claims 1-4, wherein the node (204) is a router, **characterised** by the router having means (216) for prioritising a real-time flow over non-real-time flows when routing.

10. The IP network (200) according to any of the claims 1-9, **characterised** by the real-time flow carrying RTP (Real-time Transfer Protocol) frames and the flows is a UDP (User Datagram Protocol) flow.

11. A Flow Classifier (205) for classifying whether a transmitted flow, comprising datagrams, within an IP network (200) is real-time flow or not, the Flow Classifier (205) receiving an incoming aggregated flow (201) of IP packets **characterised** by the Flow Classifier (205) having;

- means(206) for distinguishing at least one set of flow in the aggregated flow, each flow corresponding to a uni-directional packet stream from a single session,

the Flow Classifier (205) having at least one of the following means;

- means (207) for checking the payload size of the transport layer datagram of a packet in a flow of a particular session;
- means (208) for checking for static behaviour in header fields of a number of consecutive data packets in the flow of a particular session;
- means (209) for checking for an incremental behaviour of header fields, of a number of consecutive data packets in the flow of a particular session;

the Flow Classifier (205) further having:

- means for performing one of said checkings;
- means for performing a further one of the not yet performed said checkings, if said performed first checking results in that the flow possible is a real-time flow;
- means for performing a yet further one of the not yet performed said checkings and so on until all said checkings are performed,
- means for deciding that the flow is a real-time flow, if the last performed checking step results in that the flow possible is a real time flow.

12 The Flow Classifier (205) according to claim 11, **characterised** by the Flow Classifier (205) having means (212) for checking if the values of the possible

header fields of an application datagram in a flow of a particular session satisfy range restrictions of a header of an application datagram comprising real-time data.

13 The Flow Classifier (205) according to any of the claims 11-12, **characterised** by the Flow Classifier (205) having means (213) for checking if the payload size of the transport layer datagram in a flow of a particular session is at least as large as the smallest possible datagram of any application comprising real-time data.

14 The Flow Classifier (205) according to any of the claims 11-13, **characterised** by the real-time flow carrying RTP (Real-time Transfer Protocol) frames and the flow is a UDP (User Datagram Protocol) flow.

15. Method for distinguishing a real-time flow from non-real-time flows in a stream of IP packets in an IP network (200), the IP network (200) comprising a node (204) receiving an incoming aggregated flow of IP datagram, comprising the step of:

- *distinguishing* (300) at least one set of flow in the incoming aggregated flow where each distinguished flow corresponds to a uni-directional packet stream from a single session;

and performing one of the following checking steps:

- *checking* (301) the payload size of the transport layer datagram of a packet in a flow of a particular session;
- *checking* (302) if the values of the possible header fields of an application datagram in a flow of a particular session satisfy the range restrictions of a header of an application datagram comprising real-time data;
- *checking* (303) for static behaviour in header fields, of a number of consecutive data packets of a particular session;
- *checking* (304) for incremental behaviour of header fields, of a number of consecutive data packets of a particular session;

if said checking results in that the flow possible is a real-time flow,

– *performing* a further one of the not yet performed said checking steps;

if said further checking results in that the flow possible is a real-time flow,

– *performing* a further one of the not yet performed said checking steps,

and so on until all checking steps are performed;

if the last performed checking step results in that the flow possible is a real-time flow,

– *deciding* (305) that the flow is a real-time flow.

16. The method of claim 15, comprising the further step of *reporting* the decision (305) to the node (204).

17. The method according to any of the claims 15 and 16, wherein the step of checking the payload size (301) of the datagram of the transport layer comprises *checking* if payload the size of the datagram of the transport layer is at least as large as the smallest possible datagram of any session comprising real-time data.

18. The method according to any of the claims 16-17, wherein an out-going link (203) of the node (204) is a radio link, comprising the further step to be taken after reporting the decision to the node (204):

allocating at least one radio resource on basis of whether the flow is a real-time flow or not.

19. The method according to any of the claims 16-18, comprising the further step to be taken after reporting the decision to the node (204):

requesting the link layer to recover from errors if the flow is non-real-time flow.

20. The method according to any of the claims 16-18, comprising the further step to be taken after reporting the decision to the node (204):

requesting the link layer to not recover from errors if the flow is a real-time flow.

21. The method according to any of the claims 16-17, comprising the further step to be taken after reporting the decision to the node (204), the node (204) being a switch:

prioritising a real-time flow over non-real-time flows when switching.

22. The method according to any of the claims 16-17, comprising the further step to be taken after reporting the decision to the node (204), the node (204) being a router :

prioritising a real-time flow over non-real-time flows when routing.

23. The method according to any of the claims 15-22, wherein the real-time flow carries RTP (Real-time Transfer Protocol) frames and the flow is a UDP (User Datagram Protocol) flow.

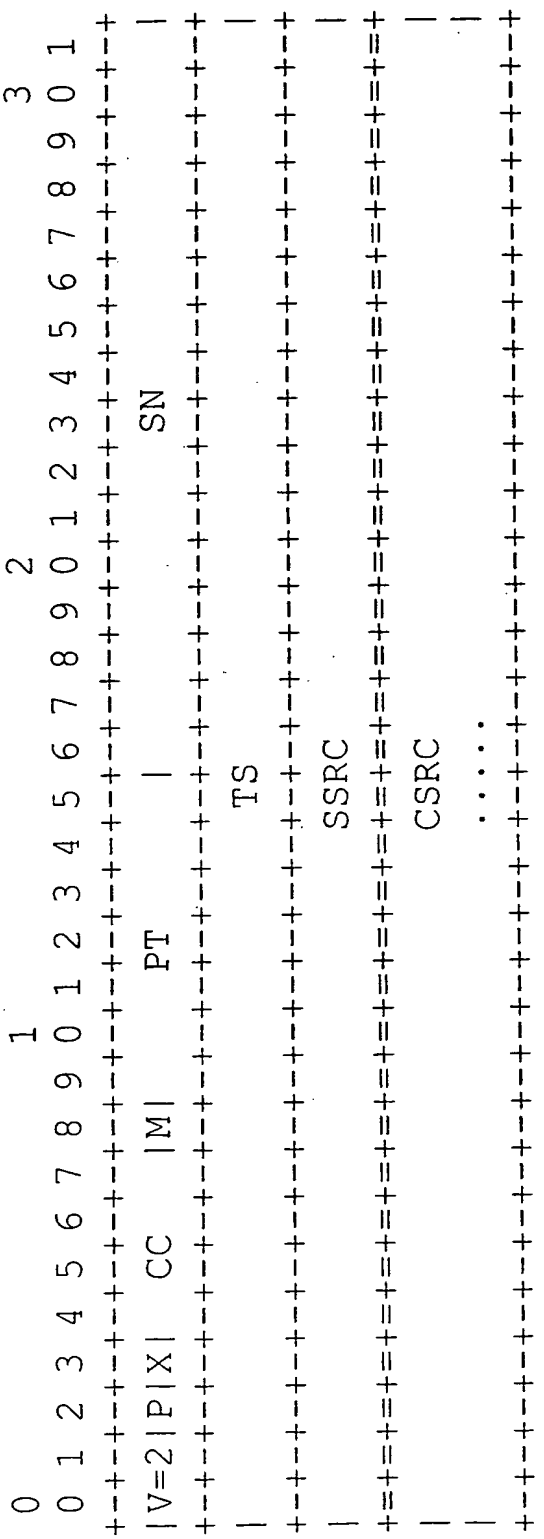


Fig. 1

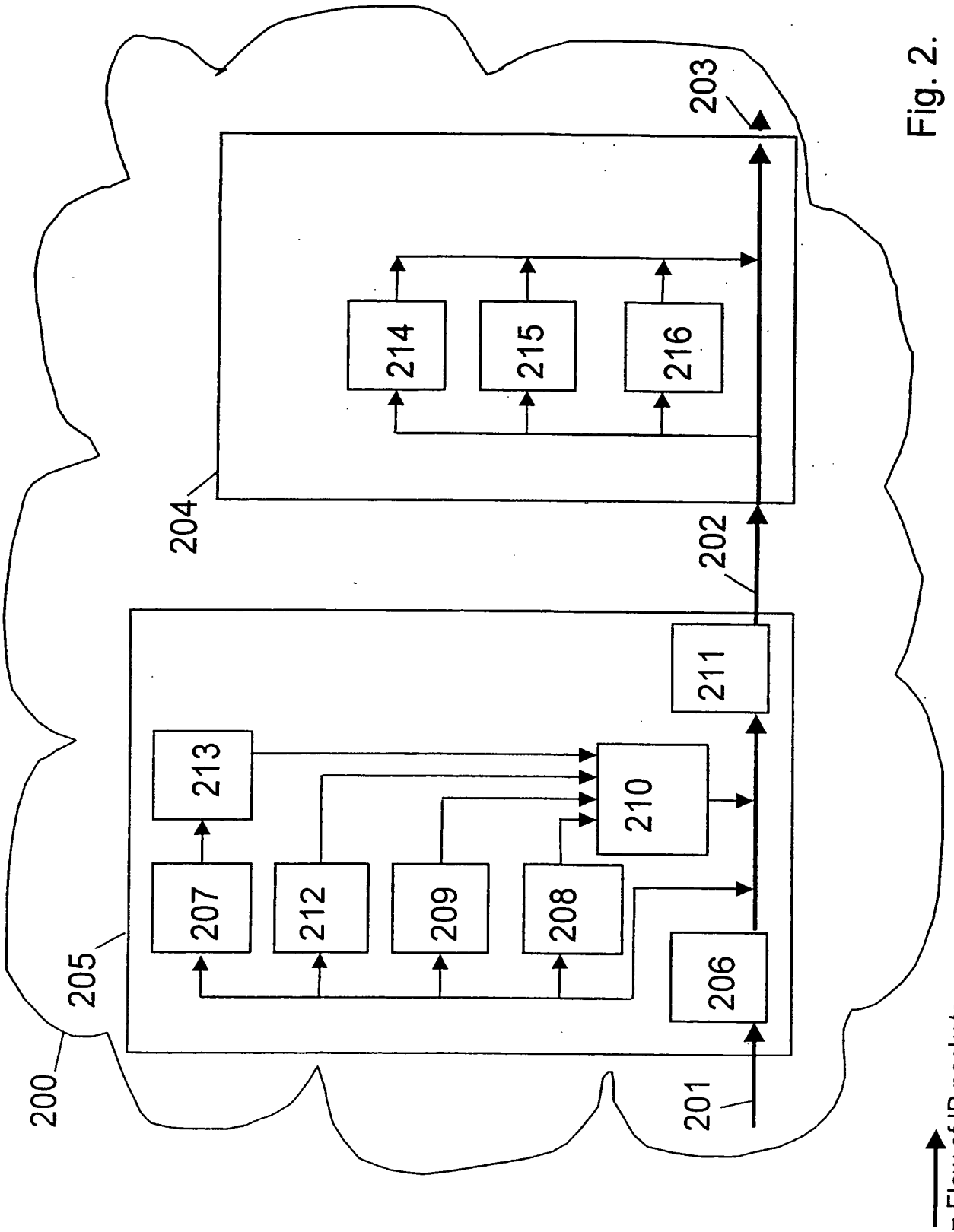


Fig. 2.

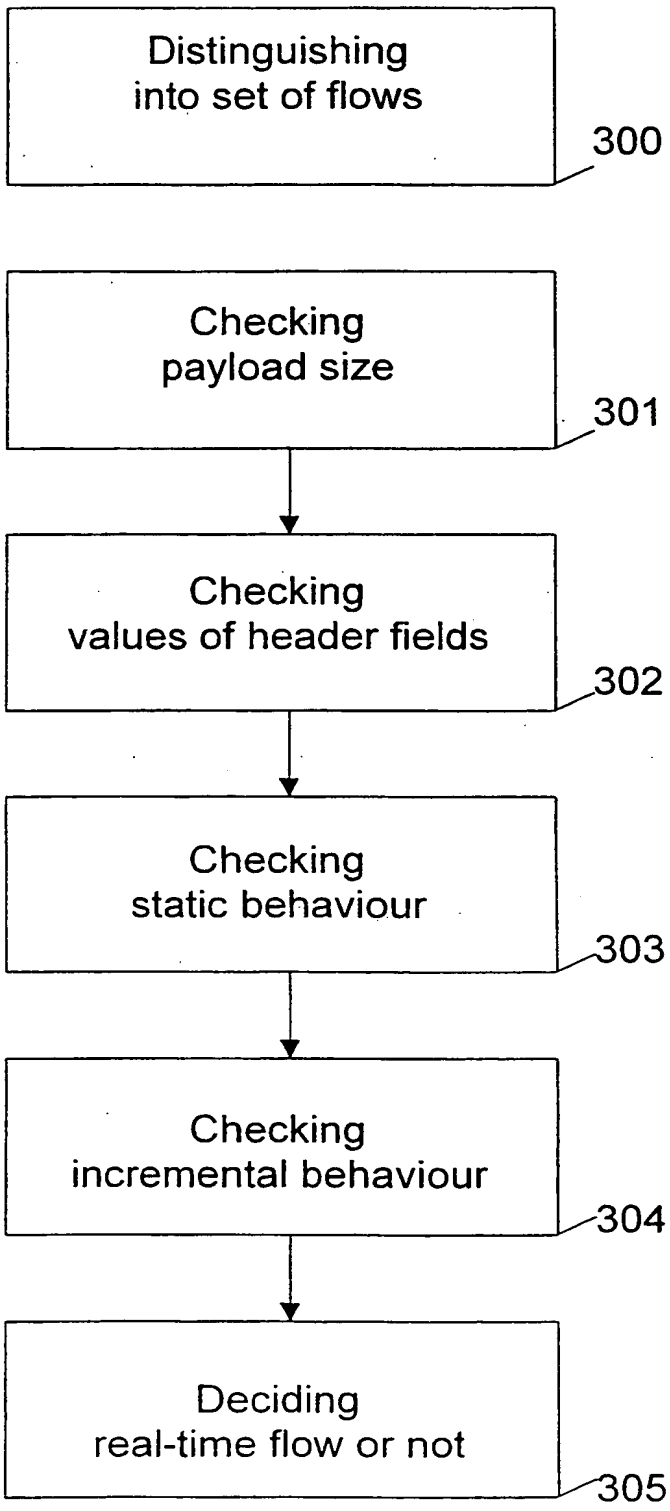


Fig. 3.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01712

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/56, H04L 29/06
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9828938 A1 (NORTHERN TELECOM LIMITED), 2 July 1998 (02.07.98), page 9, line 27 - page 10, line 25, claims 1,4,6	1-23
A	US 5574720 A (SOONG H. LEE), 12 November 1996 (12.11.96), column 4, line 13 - line 26, figure 4, abstract	1-23
A	http://www.cs. columbia.edu/~hgs/rpt .../draft-ietf-avt-germ-00.txt November 11, 1998 GeRM: Generic RTP Multiplexing Mark Handley see whole document	1-23

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 December 2000	09-01-2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rickard Elg/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

)OCID: <WO___0122666A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

04/12/00

International application No.
PCT/SE 00/01712

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9828938 A1	02/07/98	EP 0954943 A	10/11/99
		JP 2000508145 T	27/06/00
		US 6023456 A	08/02/00
		US 6028842 A	22/02/00
		WO 9828939 A	02/07/98
US 5574720 A	12/11/96	JP 2798897 B	17/09/98
		JP 7264188 A	13/10/95
		KR 9700668 B	16/01/97